Avira Server Security

User Manual

AVIRA

Trademarks and Copyright

Trademarks

Windows is a registered trademark of the Microsoft Corporation in the United States and other countries.
All other brand and product names are trademarks or registered trademarks of their respective owners.
Protected trademarks are not marked as such in this manual. This does not mean, however, that they may be used freely.

Copyright information

Code provided by third party providers was used for Avira Server Security. We thank the copyright owners for making the code available to us.
For detailed information on copyright, please refer to "Third Party Licenses" in the Program Help of Avira Server Security.

Table of Contents

1. Introduction 6
1.1 Icons and emphases 6
2. Product information 8
2.1 Functionality 8
2.2 Delivery scope 9
2.3 System requirements 10
2.4 Licensing 11
3. Installation and uninstallation 12
3.1 Installation 12
3.1.1 Installation types 12
3.2 Uninstallation 14
3.3 Installation and uninstallation on the network 14
3.3.1 Installation on the network 15
3.3.2 Uninstallation on the network 16
3.3.3 Command line parameters for the setup program 16
3.3.4 Parameters of the file setup.inf 16

4. User interface and operation 18

4.1 User interface: Avira Server Security Console 18

4.2 User interface: Tray icon 21

4.3 Quickstart 22

5. System Scanner 24

6. Updates 25

7. Viruses and more 26

7.1 Viruses and other malware 26

7.2 Threat categories 29

8. Info and Service 34

8.1 Contact address 34

8.2 Technical support 34

8.3 Suspicious file 35

8.4 Reporting false positives 35

8.5 Your feedback for more security 35

9. Reference: Configuration options 36

9.1 System Scanner 36

9.1.1 Action on detection 39

9.1.2 Further actions 41

9.1.3 Archives 41

9.1.4 Exceptions 43

9.1.5 Heuristic 44

9.1.6 Report 45

9.2 Real-Time Protection 45

9.2.1 Action on detection 48

9.2.2 Further actions 52

9.2.3 Exceptions 52

9.2.4 Products 56

9.2.5 Heuristic 56

9.2.6 Report 57

9.3 Variables: Real-Time Protection and System Scanner exceptions 59

9.3.1 Variables for Windows XP 32-Bit (**English) 59

9.3.2 Variables for Windows 7 32-Bit/ 64-Bit (**English) 60
9.4 Update 60
9.4.1 Product update 61
9.4.2 Web server 62
9.4.3 Proxy settings 62
9.5 General 63
9.5.1 Threat categories 63
9.5.2 Password 64
9.5.3 WMI 65
9.5.4 Events 65
9.5.5 Reports 65
9.5.6 Directories 66
9.6 Alerts 67
9.6.1 Real-Time Protection network alerts 68
9.6.2 System Scanner network alerts 69
9.6.3 Acoustic alerts 70
9.7 Email 71
9.7.1 Real-Time Protection email alerts 72
9.7.2 System Scanner email alerts 73
9.7.3 Updater email alerts 74
9.7.4 Email template 75

1. Introduction

Your Avira product protects your computer against viruses, worms, Trojans, adware and spyware and other risks. In this manual these are referred to as viruses or malware (harmful software) and unwanted programs.

The manual describes the program installation and operation.

For further options and information, please visit our website:
http://www.avira.com

The Avira website lets you:

- access information on other Avira desktop programs
- download the latest Avira desktop programs
- download the latest product manuals in PDF format
- download free support and repair tools
- access our comprehensive knowledge database and FAQs for troubleshooting
- access country-specific support addresses.

Your Avira Team

1.1 Icons and emphases

The following icons are used:

Icon / designation	Explanation
✓	Placed before a condition which must be fulfilled prior to execution of an action.
▸	Placed before an action step that you perform.
↪	Placed before an event that follows the previous action.
Warning	Placed before a warning when critical data loss might occur.

Note	Placed before a link to particularly important information or a tip which makes your Avira product easier to use.

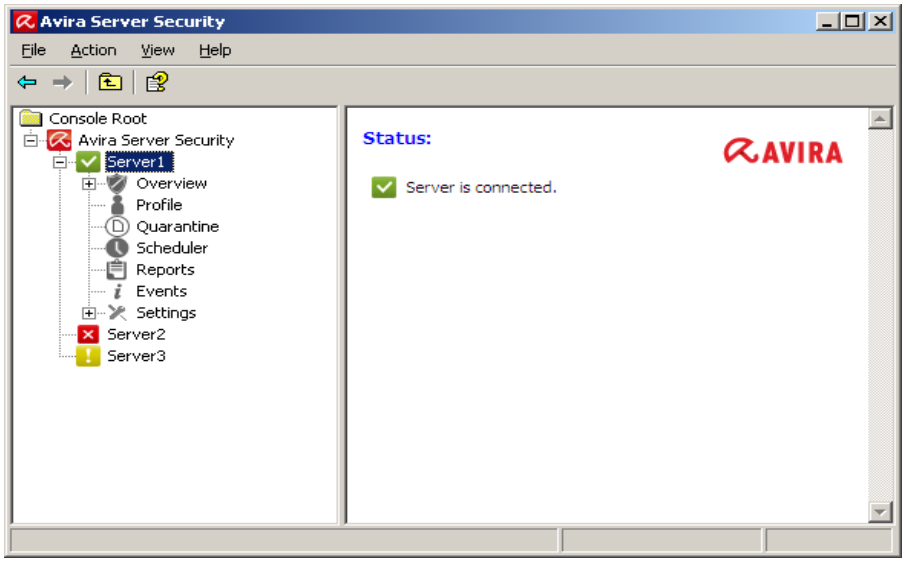
The following emphases are used:

Emphasis	Explanation
Italics	File name or path data.
	Displayed software interface elements (e.g. window section or error message).
Bold	Clickable software interface elements (e.g. menu item, navigation area, option box or button).

2. Product information

2.1 Functionality

The Avira Server Security protection package includes the Avira Server Security service and the Avira Server Security Console. The Avira Server Security service protects your Windows Server from viruses and malware. The Avira Server Security Console is used for management, control and monitoring of the servers to be protected or of the Avira Server Security services on the servers to be protected. You can access any number of servers via the Avira Server Security Console.



The Avira Server Security service

... protects your servers against viruses and malware. You install the service on all Windows servers to be protected on the network.

The Avira Server Security service provides comprehensive functions to protect your system in one package with several program components and other help programs. Overview of the main components:

- The **System Scanner** scans your computer system for viruses and unwanted programs (on-demand scan). Affected files are deleted, repaired or moved to quarantine depending on the configuration. System Scanner scans are performed automatically. The interval and scope of scans can be configured.
- The **Realtime Protection** runs in the background. It monitors and repairs files, if necessary, during operations such as opening, writing and copying in real time.
- The **Scheduler** supports you in planning regular tasks such as scans and updates via the Internet or Intranet.

- The **Updater** always keeps your program up to date via an Internet or intranet connection.
- The **Quarantine manager** conveniently manages and monitors the files placed in quarantine.

Avira Server Security Console

... provides a desktop for Avira Server Security services with which you can control, configure and monitor Avira Server Security services. You install the Avira Server Security Console on at least one computer with a network connection to the servers to be protected. Avira Server Security Console can also be installed on the servers to be protected.

The Avira Server Security Console can be connected to any number of servers to be protected and provides access to components, reports, events and to the Configuration of the connected Avira Server Security service.

2.2 Delivery scope

Main features:

- Console for monitoring, management and control of the whole program
- Simple, keyword-based configuration: support for configuration through integrated wizard and context-sensitive help
- Configuration and operation from separate computer possible: user interface (Avira Server Security Console) can be installed separately from the Avira Server Security service
- Network management via the Avira Management Console (AMC)
- System Scanner (on-demand scan) with profile-controlled and configurable scan for all known types of viruses and malware
- Resident virus guard (real-time scan or on-access scan) for constant monitoring of all file accesses
- Extremely high virus and malware detection via innovative scanning technology (scan engine) including heuristic scanning method
- Innovative AHeAD (Advanced Heuristic Analysis and Detection) technology for detection of unknown or fast changing attackers for proactive security
- Detection of all conventional archive types including detection of nested archives and smart extension detection
- Comprehensive filter functions and file caching to increase scanning speed
- "Multi-threading capability": simultaneous scanning of many files at high speed
- Configurable reactions to a detection: repair, deletion, moving to a quarantine directory, blocking, renaming and isolation of programs or files; automatic removal of viruses and malware

- Quarantine manager: infected files can be deleted in the quarantine directory or restored at their place of origin
- Integrated scheduler for planning one-off or recurring jobs such as updates or scans
- Automatable updating via the Internet or network-wide distribution (without system interruption)
- Comprehensive logging, warning and messaging functions for the administrator; sending of warnings in Windows networks and by email (SMTP), SMTP authentication possible
- Protection against modification of the program files as a result of intensive self-test
- Extended terminal server support
- Rootkits protection (not under Windows XP 64 bit, Windows 2003 64 bit, Windows Server 2003 64 bit)
- Support for Windows Management Instrumentation

2.3 System requirements

The Avira Server Security has the following requirements for successful use of the Avira Server Security service and the Avira Server Security Console:

- Computer Pentium or later, at least 1 GHz
- Operating system
  - Windows XP, newest SP (32 or 64 bit) or
  - Windows Vista (32 or 64 bit, SP1 recommended) or
  - Windows 7, newest SP (32 or 64 bit) or
  - Windows Server 2003, newest SP (32 or 64 bit) or
  - Windows Server 2008, newest SP (32 or 64 bit) or
  - Windows Server 2008 R2, newest SP (64 bit only)
- At least 150 MB of free hard disk memory space (more if using quarantine for temporary storage)
- At least 512 MB RAM (dedicated to Avira Server Security only) under Windows Server 2003
- At least 1024 MB RAM (dedicated to Avira Server Security only) under Windows Vista, Windows 7, Windows Server 2008 and Windows Server 2008 R2
- For installation of the Avira Server Security: Administrator rights
- The Avira Server Security Console is a snap-in of the Microsoft Management Console (MMC). On 64-bit operating systems, you can create an MMC snap-in only by using the MMC for 32-bit applications.

Internet access

For regular updates it is necessary for a server in your network to have Internet access. Alternatively, the updates can also be downloaded from a file or HTTP server in the Intranet. More information is available under Update.

2.4 Licensing

You require a license to use Avira Server Security. Activate your license for Avira Server Security with the license file *hbedv.key*. You can obtain the license file by email from Avira. The license file contains the license for all products that you have ordered in one order process. You thereby accept the license terms.

License models

You can use the many functions of Avira Server Security with the following license models:

- Evaluation version: Complete range of functions, 30-day license.
- Full version

Licensing comprises a license for all platforms and depends on the number of users in the network who are to be protected by Avira Server Security. For further information on the licensing versions and the optional support offers, please go to our website:
http://www.avira.com

The delivery scope of a full version comprises:

- provision of Avira version to download from the Internet
- four weeks installation support from date of purchase
- newsletter service (by email)
- update service via Internet

3. Installation and uninstallation

3.1 Installation

Before installing Avira Server Security, certain conditions must be met:

- ✓ Please ensure that the system requirements are met (see System requirements), and that the Windows Server used is running.
- ✓ Ensure that you are logged in on the server as an administrator or as a user with administrator rights.
- ✓ Ensure that an Internet connection or network connection to a download server exists for updating the Avira Server Security. If you use a fileserver, you may require a user name and a password for server login.
- ✓ When installing the full version: ensure that a valid license file *hbedv.key* exists and is stored in a local directory on the server.
- ✓ When installing the service Avira Server Security: If you want to connect remotely to the protected server with the Avira Server Security Console, ensure that the following ports are opened:
  139 (NetBIOS SSN)
  137 (NetBIOS NS)
  138 (NetBIOS DGM)

> Note
> When installing on a server operating system, the Real-Time Protection and the files protection are not available.

3.1.1 Installation types

During installation you can select a setup type in the installation wizard:

Express

- Avira Server Security is installed together with the Avira Server Security service, the Avira Server Security Console and all recommended program components.
- No destination folder can be selected for the program files to be installed.

User-defined

- You can select whether you want to install the Avira Server Security service and/or the Avira Server Security Console.
- You have the option to select and install additional functions for the Avira Server Security service:
  Avira Rootkits Protection: This function contains the rootkit scan profile, which you can use to look for hidden malware.

VMware Offline System Scanner: This function contains the VMware-Image scan profile, which you can use to perform an offline scan of VMware images for viruses and unwanted programs.
Shell Extension: This function generates an entry in the context menu of Windows Explorer that can be used to scan directories for viruses and unwanted programs.

- A target folder can be selected for the program files to be installed.

Performing installation

Installing the Avira Server Security:

- Start the setup by double-clicking the installation file that you have downloaded from the Internet or insert the program CD.
  - ↪ The installation wizard opens.
- Follow the instructions of the installation wizard. Complete the following installation steps:
- Where appropriate, install Microsoft Visual C++ 2008 - Redistributable Kit, if the kit has not already been installed.

> **Note**
> Avira Server Security uses the runtime libraries of the Microsoft Visual C++ 2008 - Redistributable Kit. To use the Avira Server Security, Microsoft Visual C++ 2008 - Redistributable Kit must be installed.

- Confirmation of license agreements
- Selection of the type of setup (express installation or user-defined installation)
- Licensing of the Avira Server Security: Load the license file or select a 30-day test license
- Installation of Avira Server Security service and/or Avira Server Security Console
- If you have installed the Avira Server Security service, a configuration wizard opens after the installation has been completed.
  - ↪ You have the option of configuring the most important settings of the installed Avira Server Security service.
- **Defining AHeAD (Advanced Heuristic Analysis and Detection) technology settings:** The settings are defined for System Scanner and Real-Time Protection.
- **Selection of extended threat categories:** By selecting other extended threat categories to be detected and reported by the Avira Server, you can adapt the protective function of the Avira Server Security to meet your needs.
- **Selection of product exceptions (Real-Time Protection):** You can select software products to be exempt from monitoring by the Real-Time Protection (on-access System Scanner). In this way you can avoid any loss of performance that the Real-Time Protection may cause.

- **Select email settings:** You can define the server settings for sending email. Avira Server Securityuses SMPT to send emails send email alerts to the Avira Server Security administrator.

Note
After installation, your own system is automatically added by the Avira Server Security Console (Local Host/127.0.0.1) as a server to be protected, even if no Avira Server Security service is installed.

Note
If you want to add or remove program components of the current Avira Server Security installation, use the Avira Server Security setup.

3.2 Uninstallation

Carry out uninstallation via the Control Panel of the operating system or via the setup of your Avira product.

During uninstallation, the Avira services are stopped, all report files and infected files (in quarantine) are deleted.

During uninstallation you can specify that the directories with the report files and the quarantine are not deleted.

You will be asked to restart your computer.

- Click **Yes** to confirm.
  - ↪ Your Avira product is uninstalled now.

3.3 Installation and uninstallation on the network

To simplify installation of Avira products on a network of multiple client computers for the system administrator, your Avira product has a special procedure for the initial installation and the change installation.

For automatic installation, the setup program works with the control file *setup.inf*. The setup program (*presetup.exe*) is contained in the program's installation package. Installation is started with a script or batch file and all necessary information is obtained from the control file. The script commands therefore replace the usual manual inputs during installation.

Note
Please note that a license file is obligatory for initial installation on the network.

Note
Please note that an installation package for the Avira product is required for installation via a network. An installation file for Internet-based installation cannot be used.

Avira products can be easily shared on the network with a server login script or via SMS.

For information on installation and uninstallation on the network:

- see Chapter: Command line parameters for the setup program
- see Chapter: Parameter of the file *setup.inf*
- see Chapter: Installation on the network
- see Chapter: Uninstallation on the network

3.3.1 Installation on the network

The installation can be script-controlled in batch mode.

The setup is suitable for the following installation:

- Initial installation via the network (unattended setup)
  - Change installation and update

Note
We recommend that you test automatic installation before the installation routine is implemented on the network.

Note
When installing on a server operating system, the Real-Time Protection and the files protection are not available.

To install Avira product on the network automatically:

✓ You must have administrator rights (also required in batch mode)

- Configure the parameter of the file *setup.inf* and save the file.
- Begin installation with the parameter /inf or integrate the parameter into the login script of the server.

Example: `presetup.exe /inf="c:\temp\setup.inf"`

3.3.2 Uninstallation on the network

To uninstall Avira products on the network automatically:

✓ You must have administrator rights (also required in batch mode)

Example: `presetup.exe /remsilent /unsetuplog="c:\logfiles\unsetup.log"`

▸ Start the uninstallation with the parameters `/inf and /AVUNINSTALL` or integrate the parameters into the login script of the server.

3.3.3 Command line parameters for the setup program

Use the following parameters for installation and uninstallation:

- `/INF=<Script name with path>`

  The setup program starts with the script mentioned and retrieves all parameters required.
  Installation: `PRESETUP.EXE /INF=e:\disks\setup.inf`
  Uninstallation: `PRESETUP.EXE /INF=e:\disks\setup.inf /AVUNINSTALL`

- /SILENT

  The setup script runs down completely without user interaction.

3.3.4 Parameters of the file setup.inf

In the control file *setup.inf*, you can set the following parameters in the [DATA] field for the automatic installation of the Avira product. The sequence of the parameters is unimportant. If a parameter setting is missing or wrong, the setup routine is aborted and an error message is displayed.

- `InstallPath`

  Destination path in which the Avira Server Security is installed. It has to be included to the script. The environment variable cannot be used.
  Example: InstallPath="%PROGRAMFILES%\Avira\AntiVir Server\"

- `LicenseFile=<Path and file name of the license file>`

  Avira Server Security is installed with the license. If you enter the file name only, the license file will be searched in the source folder of the setup only.
  Example: `LicenseFile="A:\hbedv.key"`

- `RestartWindows= 0 | 1`

  If a restart of the system is required after the installation, this can be performed automatically (standard) or a message box is displayed.
  `0`: Disabled (restart with Message Box)
  `1`: Enabled (automatic restart)

- `DeleteFolderOnUninstall=1`

  Deletes the configuration during uninstallation

- `Guard= 0 | 1`

  Installs the Avira Real-Time Protection (on-access Scanner).
  1: Install Avira Real-Time Protection (default)
  0: Do not install Avira Real-Time Protection

- `RootKit= 0 | 1`

  Installs the AntiVir rootkit protection module. The module detects malware hidden in the system.
  1: Install AntiVir Rootkits Protection
  0: Do not install AntiVir Rootkits Protection (default)

- `VMWare= 0 | 1`

  Installs the VMWare offline Scanner. The module performs an offline scan of VMWare images for viruses and malware.
  1: Install VMWare offline Scanner
  0: Do not install VMWare offline Scanner (default)

- `ShellExtension= 0 | 1`

  Installs the Shell extension. Directories can be scanned directly for viruses and unwanted programs using an entry in the Windows Explorer context menu.
  1: Install Shell extension (default)
  0: Do not install Shell extension

- `Systray= 0 | 1`

  Installs the Systray tool. An Avira Server Security tray icon is visible in the notification area of the protected server. The Tray Icon lets you monitor the status of the Avira Server Security and gives you access to other Avira Server Security functions.
  1: Install Systray tool (default)
  0: Do not install Systray tool

- `GUI= 0 | 1`

  Installs the Avira Server Security Console user interface, which allows you to remotely manage and configure the Avira Server Security services running on protected servers.
  1: Installs the Avira Server Security Console (default)
  0: Does not install the Avira Server Security Console

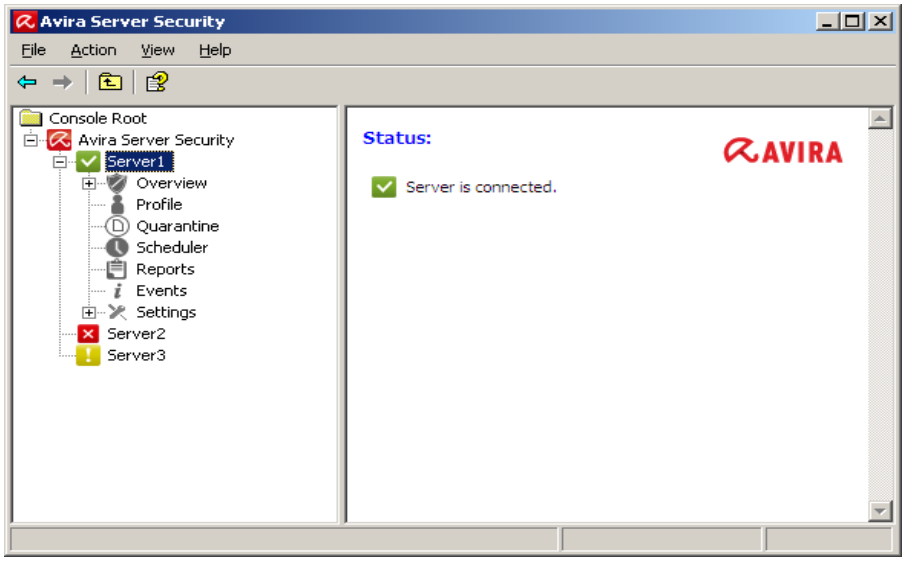
In the [FEEDBACK] section the setup enters error codes and error test which are reported by the setup:

Example: `ErrCode=0`
`ErrMsg=Product was installed successfully`

4. User interface and operation

4.1 User interface: Avira Server Security Console

The Avira Server Security service that is installed on the servers to be protected is managed via the **Avira Server Security Console**. The Avira Server Security Console is a snap-in of the Microsoft Management Console (MMC). You can create any number of servers to be protected on the Avira Server Security Console in order to configure and monitor them on the Avira Server Security Console.



Note
Please note that only the proprietary elements of the Avira Server Security Console are documented in this help. For information on the MMC and on manual integration of a snap-in, please refer to the user manual or the online help of the operating system.

Starting and closing the Avira Server Security Console

Start the Avira Server Security Console via the **Avira Server Security user interface** link in the Windows Start menu or under **All programs**. You can also load the Avira Server Security Console directly in the MMC. You will find the preconfigured Avira Server Security Console in the installation directory of the Avira Server Security Console. To close the Avira Server Security Console, you must close MMC.

Operation

- Navigate via the console structure in the left-hand window of the MMC.

Navigation elements are also displayed as objects in the right-hand detail window of the MMC. Open these objects in the detail window by double-clicking.

The Configuration is located under the node **Settings**. Expand the node and click the module you would like to configure.

↪ You can select various configuration sections in the detail window:

- Commands and actions are available via icons in the detail window and via context menus of the individual console nodes or of objects in the detail window.
- When configuring a server, you must confirm information in the window **Settings** with the button **OK** or **Accept** in order to accept the new settings. Your settings are cancelled with the button **Cancel**.

Avira Server Security Console overview

Avira Server Security

- Display of the created servers with connection status
- Actions: **Add server**

> **Note**
> The local Avira server and all Avira severs added by the registered user are displayed on the Avira Server Security Console.

Server

- Display of server status
- Actions:
  - **start product update**
  - **update license file**
  - **reload configuration**
  - **display report file**
  - **rename server**
  - **disconnect server**
  - **connect server**
  - **delete server**

Overview

- system status (last system test, last update, license)
- statistical data of the on-access scan of the Real-Time Protection and the on-demand scan of the System Scanner
- program version

- contact and support addresses

Profiles

- Display of the default profiles and of the profiles created for the on-demand scan
- Actions:
  - **create new profiles**
  - **rename profiles**
  - **delete profiles**

Quarantine

- Display of the objects in quarantine
- Actions:
  - **scan object again**
  - **display object properties**
  - **restore object**
  - **add file to quarantine**
  - **send object to Avira Malware Research Center**
  - **delete object**
  - **export all properties**

Scheduler

- Display of all created scanning and update jobs
- Actions:
  - **insert new jobs**
  - **display job properties**
  - **edit job**
  - **delete job**

Reports

- Display reports of scans of on-demand scan and updates
- Actions:
  - **display report**
  - **display report file**
  - **print report**
  - **delete report**

Events

- Display all events of the Avira Server Security service on the server to be protected
- Actions:
  - **display events**
  - **export events**
  - **delete events**

Settings

- Configuration of the Avira Server Security service on the server to be protected
- Configuration sections:
  - **System Scanner**: Configuration of on-demand scan
  - **Realtime Protection**: Configuration of on-access scan
  - **General**: Extended risk categories for on-demand and on-access scans, password protection for the server on the Avira Server Security Console, security alerts for outdated Avira servers, directories used, restriction of reports and of event log
  - **Update**: Download via web server or file server, product updates, configuration of connection to the download server
  - **Alerts**: Configuration of network alerts of the Real-Time Protection and System Scanner
  - **Email**: Configuration of email alerts via SMTP from the Real-Time Protection, System Scanner, Updater modules

4.2 User interface: Tray icon

After installation of the Avira Server Security service, the Avira Server Security tray icon is displayed on the protected server in the notification area. The tray icon displays the status of the Avira Real-Time Protection:

Icon	Description
	Avira Real-Time Protection is enabled
	Avira Real-Time Protection is disabled

You can access the functions via the tray icon context menu.

- To open the context menu, click the tray icon with the right-hand mouse button.

- **Start Avira**: Opens the Avira Server Security Console for management of the connected Avira Server. This option is only available if an Avira Server Security

Console has been installed locally on the computer and if you are logged on to the computer with administrator rights.

- Check **My Documents**: Starts the System Scanner scan profile **My Documents**: The default **My files** location of the logged-in user is scanned for viruses and unwanted programs.
- **Help**: opens the Online Help.
- **Avira on the Internet**: Opens the Avira web portal.

> **Note**
> The Avira Server Security Console can also be opened by double-clicking the tray icon.

4.3 Quickstart

Carry out these steps if you are using the Avira Server Security for the first time:

1. Installation

Install the Avira Server Security service on the servers that you want to protect against viruses and unwanted programs. Install the Avira Server Security Console on at least one computer on your network.
See chapter Installation.

2. Management on the Avira Server Security Console

- **Add server**

  Add all servers on the Avira Server Security Console that you want to manage on the Avira Server Security Console.
  See Chapter Avira Server Security Console.

Carry out the following steps for every server added:

- **Configuration**

  Configure the Avira Server Security service on the server to be protected. Assign a password for the server on the Avira Server Security Console.
  See Chapters Settings and Settings > General > Password.

- **Carry out update and system scan**

  First carry out an update. For this, create an update job in the **Scheduler**. Select "Immediately" as the start time. Carry out a complete system scan. For this, create a scan job in the **Scheduler**. For the scan job, select "Local hard disks" as the profile

and "Immediately" as the start time.
See Chapter Scheduler.

- **Define scans and update jobs**

  Define scans and update jobs. To configure Scanner scans, first create, where appropriate, user-defined profiles under **Scheduler** In the next step you can create the scans and update jobs under **Scheduler**.
  See Chapters Scan and Scheduler.

5. System Scanner

With the Scanner component, you can carry out targeted scans (on-demand scans) for viruses and unwanted programs. The following options are available for scanning for infected files:

- **Scan in Scheduler (remote and local)**
  The Scheduler gives you the option to schedule the times at which scan jobs are to be executed on the protected server.
- **Scan via Profile (remote and local)**
  Profiles enable you to initiate defined and configured scan profiles on the protected server.
- **Shell Extension: Scan from the context menu in Windows Explorer (local only)**
  You have the option to use the **Scan selected files with Avira** entry in the context menu of a directory to scan that directory for viruses and unwanted programs. The **Shell Extension** function is an additional component that is only available if it was selected during the user-defined installation.
- **Scanning of own documents using the context menu of the tray icon (local only)**
- You can initiate a scan for viruses and unwanted programs in the Windows *'My files'* user directory of the protected server by choosing the **My Documents** entry in the tray icon context menu.

Special processes are required when scanning for rootkits, boot sector viruses, and when scanning active processes. The following options are available:

- Scan for rootkits via the scan profile *Scan for Rootkits and active malware*
- Scan active processes via the scan profile *Active processes*
- Scan for boot sector viruses in all scan profiles by activating the corresponding options under **Settings > System Scanner > Scan: Additional settings**

6. Updates

The effectiveness of anti-virus software depends entirely on the scanning engine and the virus definitions being up-to-date. For this reason, regularly download updates for the Avira Server Security from our download servers. To enable regular updates to be performed, the Updater component is integrated in the Avira Server Security. The Updater component updates the following program components:

- Virus definition file
- Scan engine
- Program files (product update)

The Scheduler facility on the Avira server console allows you to create update jobs that will be executed by Avira Updater at the specified intervals. Following the installation of Avira server, an update job is created that will be executed by default at the following interval: 60 minutes.

With every update order, the status of the virus definition files and the scan engine is checked and updated if necessary, product updates are performed in accordance with the configuration. You can initiate a manual product update from the context menu of a server node on the Avira Server Security Console. A restart of the system after an update is required only after a product update.

You can obtain updates via the following servers:

- directly from the **Internet** via a **web server of Avira**
- via a **web server or file server on an intranet**, which downloads the update files from the Internet as the master server and supplies them to other servers. This is useful if you want to update Avira Server Security on more than one computer on a network. A download server on an intranet can be used to ensure the Avira Server Security is up-to-date on the protected servers using a minimum of resources. To set up a functioning download server on an intranet, you need a server that is compatible with the update structure of the Avira Server Security.

When a web server is used, the HTTP protocol is used for the download. When using a file server, access to the update file is provided via the network. The update is configured on the Avira Server Security Console.

> **Note**
> You can use Avira Update Manager (file server or web server in Windows) as a web server or file server in the intranet. Avira Internet Update Manager mirrors the download servers of Avira products (including the Avira Server Security) and can be obtained on the Internet from the Avira website: http://www.avira.com

7. Viruses and more

Avira Server Security not only detects viruses and malware, it can also protect you from other threats. In this chapter you can find an overview of different kinds of malware and other threats describing their background, behavior and the unpleasant surprises they have in store for you.

Related topics:

- Threat categories
- Viruses and other malware

7.1 Viruses and other malware

Adware

Adware is software that presents banner ads or in pop-up windows through a bar that appears on a computer screen. These advertisements usually cannot be removed and are consequently always visible. The connection data allow many conclusions on the usage behavior and are problematic in terms of data security.

Backdoors

A backdoor can gain access to a computer by bypassing the computer access security mechanisms.

A program that is being executed in the background generally enables the attacker almost unlimited rights. User's personal data can be spied with the backdoor's help.. But are mainly used to install further computer viruses or worms on the relevant system.

Boot viruses

The boot or master boot sector of hard disks is mainly infected by boot sector viruses. They overwrite important information necessary for the system execution. One of the awkward consequences: the computer system cannot be loaded any more…

Bot-Net

A bot-net is defined as a remote network of PCs (on the Internet) that is composed of bots that communicate with each other. A bot-net can comprise a collection of cracked machines running programs (usually referred to as worms, Trojans) under a common command and control infrastructure. Bot-nets serve various purposes, including denial-of-service attacks etc., usually without the affected PC user's knowledge. The main potential

of bot-nets is that the networks can achieve grow to thousands of computers and their total bandwidth exceeds most conventional Internet accesses.

Exploit

An exploit (security gap) is a computer program or script that takes advantage of a bug, glitch or vulnerability leading to privilege escalation or denial of service on a computer system. One form of exploitation for example is an attack from the Internet with the help of manipulated data packages. Programs can be infiltrated in order to obtain higher access.

Fraudulent software

Also known as "scareware" or "rogueware", it is a fraudulent software that pretends that your computer is infected by viruses or malware. This software looks deceptively similar to professional Antivirus software but is meant to raise uncertainty or to scare the user. Its purpose is to make the victims feel threatened of imminent (unreal) danger and to make them pay to eliminate it. There are also cases when the victims are lead to believe they were attacked and they are instructed to carry out an action, which in reality is the real attack.

Hoaxes

For several years, Internet and other network users have received alerts about viruses that are purportedly spread via email. These alerts are spread via email with the request that they should be sent to the highest possible number of colleagues and to other users, in order to warn everyone against the "danger".

Honeypot

A honeypot is a service (program or server) installed in a network. Its function is to monitor a network and log attacks. This service is unknown to the legitimate user - because of this reason he is never addressed. If an attacker examines a network for the weak points and uses the services which are offered by a honeypot, it is logged and an alert is triggered.

Macro viruses

Macro viruses are small programs that are written in the macro language of an application (e.g. WordBasic under WinWord 6.0) and that can normally only spread within documents of this application. Because of this, they are also called document viruses. In order to be active, they need that the corresponding applications are activated and that one of the infected macros has been executed. Unlike "normal" viruses, macro viruses consequently do not attack executable files but they do attack the documents of the corresponding host application.

Pharming

Pharming is a manipulation of the host file of web browsers to divert enquiries to spoofed websites. This is a further development of classic phishing. Pharming fraudsters operate their own large server farms on which fake websites are stored. Pharming has established itself as an umbrella term for various types of DNS attacks. In the case of a manipulation of the host file, a specific manipulation of a system is carried out with the aid of a Trojan or virus. The result is that the system can now only access fake websites, even if the correct web address is entered.

Phishing

Phishing means angling for personal details of the Internet user. Phishers generally send their victims apparently official letters such as emails that are intended to induce them to reveal confidential information to the culprits in good faith, in particular user names and passwords or PINs and TANs of online banking accounts. With the stolen access details, the phishers can assume the identities of the victims and carry out transactions in their name. What is clear is that: banks and insurance companies never ask for credit card numbers, PINs, TANs or other access details by email, SMS or telephone.

Polymorph viruses

Polymorph viruses are the real masters of disguise. They change their own programming codes - and are therefore very hard to detect.

Program viruses

A computer virus is a program that is capable of attaching itself to other programs after being executed and cause an infection. Viruses multiply themselves unlike logic bombs and Trojans. In contrast to a worm, a virus always requires a program as host, where the virus deposits its virulent code. The program execution of the host itself is not changed as a rule.

Rootkits

A rootkit is a collection of software tools that are installed after a computer system has been infiltrated to conceal logins of the infiltrator, hide processes and record data - generally speaking: to make themselves invisible. They attempt to update already installed spy programs and reinstall deleted spyware.

Script viruses and worms

Such viruses are extremely easy to program and they can spread - if the required technology is on hand - within a few hours via email round the globe.

Script viruses and worms use one of the script languages, such as Javascript, VBScript etc., to insert themselves in other, new scripts or to spread themselves by calling operating system functions. This frequently happens via email or through the exchange of files (documents).

A worm is a program that multiplies itself but that does not infect the host. Worms cannot consequently form part of other program sequences. Worms are often the only possibility to infiltrate any kind of damaging programs on systems with restrictive security measures.

Spyware

Spyware are so called spy programs that intercept or take partial control of a computer's operation without the user's informed consent. Spyware is designed to exploit infected computers for commercial gain.

Trojan horses (short Trojans)

Trojans are pretty common nowadays. Trojans include programs that pretend to have a particular function, but that show their real image after execution and carry out a different function that, in most cases, is destructive. Trojan horses cannot multiply themselves, which differentiates them from viruses and worms. Most of them have an interesting name (SEX.EXE or STARTME.EXE) with the intention to induce the user to start the Trojan. Immediately after execution they become active and can, for example, format the hard disk. A dropper is a special form of Trojan that 'drops' viruses, i.e. embeds viruses on the computer system.

Zombie

A zombie PC is a computer that is infected with malware programs and that enables hackers to abuse computers via remote control for criminal purposes. On command, the affected PC starts denial-of-service (DoS) attacks, for example, or sends spam and phishing emails.

7.2 Threat categories

Adware

Adware is software that presents banner ads or in pop-up windows through a bar that appears on a computer screen. These advertisements usually cannot be removed and are consequently always visible. The connection data allow many conclusions on the usage behavior and are problematic in terms of data security.

Your Avira product detects Adware. If the **Adware** option is enabled with a check mark in the configuration under Threat categories, you receive a corresponding alert if your Avira product detects adware.

Adware/Spyware

Software that displays advertising or software that sends the user's personal data to a third party, often without their knowledge or consent, and for this reason may be unwanted.

Your Avira product recognizes "Adware/Spyware". If the option **Adware/Spyware** is enabled with a check mark in the configuration under Threat categories, you receive a corresponding alert if your Avira product detects adware or spyware.

Application

The term APPL, respectively application, refers to an application which may involve a risk when used or is of dubious origin.

Your Avira product recognizes "Application (APPL)". If the option **Application** is enabled with a check mark in the configuration under Threat categories, you receive a corresponding alert if your Avira product detects such behavior.

Backdoor Clients

In order to steal data or manipulate computers, a backdoor server program is smuggled in unknown to the user. This program can be controlled by a third party using backdoor control software (client) via the Internet or a network.

Your Avira product recognizes "Backdoor control software". If the **Backdoor control software** option is enabled with a check mark in the configuration under Threat categories, you receive a corresponding alert if your Avira product detects such software.

Dialer

Certain services available in the Internet have to be paid for. They are invoiced in Germany via dialers with 0190/0900 numbers (or via 09x0 numbers in Austria and Switzerland; in Germany, the number is set to change to 09x0 in the medium term). Once installed on the computer, these programs guarantee a connection via a suitable premium rate number whose scale of charges can vary widely.

The marketing of online content via your telephone bill is legal and can be of advantage to the user. Genuine dialers leave no room for doubt that they are used deliberately and intentionally by the user. They are only installed on the user's computer subject to the user's consent, which must be given via a completely unambiguous and clearly visible labeling or request. The dial-up process of genuine dialers is clearly displayed. Moreover, genuine dialers tell you the incurred costs exactly and unmistakably.

Unfortunately there are also dialers which install themselves on computers unnoticed, by dubious means or even with deceptive intent. For example they replace the Internet user's default data communication link to the ISP (Internet Service Provider) and dial a cost-incurring and often horrendously expensive 0190/0900 number every time a connection is made. The affected user will probably not notice until his next phone bill that an unwanted

0190/0900 dialer program on his computer has dialed a premium rate number with every connection, resulting in dramatically increased costs.

We recommend that you ask your telephone provider to block this number range directly for immediate protection against undesired dialers (0190/0900 dialers).

Your Avira product can detect the familiar dialers by default.

If the option **Dialers** is enabled with a check mark in the configuration under Threat categories, you receive a corresponding alert if a dialer is detected. You can now simply delete the potentially unwanted 0190/0900 dialer. However, if it is a wanted dial-up program, you can declare it an exceptional file and this file is then no longer scanned in future.

Double Extension Files

Executable files that hide their real file extension in a suspicious way. This camouflage method is often used by malware.

Your Avira product recognizes "Double Extension Files". If the option **Double Extension files** is enabled with a check mark in the configuration under Threat categories, you receive a corresponding alert if your Avira product detects such files.

Fraudulent software

Also known as "scareware" or "rogueware", it is a fraudulent software that pretends that your computer is infected by viruses or malware. This software looks deceptively similar to professional antivirus software but is meant to raise uncertainty or to scare the user. Its purpose is to make the victims feel threatened of imminent (unreal) danger and to make them pay to eliminate it. There are also cases when the victims are lead to believe they were attacked and they are instructed to carry out an action, which in reality is the real attack.

Your Avira product detects scareware. If the option **Fraudulent software** is enabled with a check mark in the configuration Threat categories, you receive a corresponding alert if your Avira product detects such files.

Games

There is a place for computer games - but it is not necessarily at work (except perhaps in the lunch hour). Nevertheless, with the wealth of games downloadable from the Internet, a fair bit of mine sweeping and Patience playing goes on among company employees and civil servants. You can download a whole array of games via the Internet. Email games have also become more popular: numerous variants are circulating, ranging from simple chess to "fleet exercises" (including torpedo combats): The corresponding moves are sent to partners via email programs, who answer them.

Studies have shown that the number of working hours devoted to computer games has long reached economically significant proportions. It is therefore not surprising that more

and more companies are considering ways of banning computer games from workplace computers.

Your Avira product recognizes computer games. If the **Games** option is enabled with a check mark in the configuration under Threat categories, you receive a corresponding alert if your Avira product detects a game. The game is now over in the truest sense of the word, because you can simply delete it.

Jokes

Jokes are merely intended to give someone a fright or provide general amusement without causing harm or reproducing. When a joke program is loaded, the computer will usually start at some point to play a tune or display something unusual on the screen. Examples of jokes are the washing machine in the disk drive (DRAIN.COM) or the screen eater (BUGSRES.COM).

But beware! All symptoms of joke programs may also originate from a virus or Trojan. At the very least users will get quite a shock or be thrown into such a panic that they themselves may cause real damage.

Thanks to the extension of its scanning and identification routines, your Avira product is able to detect joke programs and eliminate them as unwanted programs if required. If the option **Jokes** is enabled with a check mark in the configuration under Threat categories, a corresponding alert is issued if a joke program is detected.

Phishing

Phishing, also known as "brand spoofing" is a clever form of data theft aimed at customers or potential customers of Internet service providers, banks, online banking services, registration authorities.
When submitting your email address on the Internet, filling in online forms, accessing newsgroups or websites, your data can be stolen by "Internet crawling spiders" and then used without your permission to commit fraud or other crimes.

Your Avira product recognizes "Phishing". If the option **Phishing** is enabled with a check mark in the configuration under Threat categories, you receive a corresponding alert if your Avira product detects such behavior.

Programs that violate the private domain

Software that may be able to compromise the security of your system, initiate unwanted program activities, damage your privacy or spy on your user behavior and could therefore be unwanted.

Your Avira product detects "Security Privacy Risk" software. If the option **Programs that violate the private domain** is enabled with a check mark in the configuration under Threat categories, you receive a corresponding alert if your Avira product detects such software.

Unusual Runtime Packers

Files that have been compressed with an unusual runtime packer and that can therefore be classified as potentially suspicious.

Your Avira product recognizes "Unusual runtime packers". If the option **Unusual runtime packers** is enabled with a check mark in the configuration under Threat categories, you receive a corresponding alert if your Avira product detects such packers.

8. Info and Service

This chapter contains information on how to contact us.

- see Chapter Contact address
- see Chapter Technical support
- see Chapter Suspicious files
- see Chapter Report false positives
- see Chapter Your feedback for more security

8.1 Contact address

If you have any questions or requests concerning the Avira product range, we will be pleased to help you. For our contact addresses, please refer to the Control Center under **Help > About Avira Server Security**.

8.2 Technical support

Avira support provides reliable assistance in answering your questions or solving a technical problem.

All necessary information on our comprehensive support service can be obtained from our website:

http://www.avira.de/en/support

So that we can provide you with fast, reliable help, you should have the following information ready:

- **License information**. You can find this information in the program interface under the menu item **Help > About Avira Server Security > License information**. See License information.
- **Version information**. You can find this information in the program interface under the menu item **Help > About Avira Server Security > Version information**. See Version information.
- **Operating system version** and any Service Packs installed.
- **Installed software packages**, e.g. anti-virus software of other vendors.
- **Exact messages** of the program or of the report file.

8.3 Suspicious file

Suspect files or viruses that may not yet be detected or removed by our products can be sent to us. We provide you with several ways of doing this.

- Identify the file in the quarantine manager of the Avira Server Security Console and select the item **Send file** via the context menu or the corresponding button.
- Send the required file packed (WinZIP, PKZip, Arj, etc.) in the attachment of an email to the following address:
  virus@avira.com
  As some email gateways work with anti-virus software, you should also provide the file(s) with a password (please remember to tell us the password).
- You can also send us the suspicious file via our website: http://www.avira.com/sample-upload

8.4 Reporting false positives

If you believe that your Avira product is reporting a detection in a file that is most likely "clean", send the relevant file packed (WinZIP, PKZip, Arj, etc.) as an email attachment to the following address:

virus@avira.com

As some email gateways work with anti-virus software, you should also provide the file(s) with a password (please remember to tell us the password).

8.5 Your feedback for more security

At Avira, our customers' security is paramount. For this reason, we don't just have an in-house expert team that tests the quality and security of every Avira solution before the product is released. We also attach great importance to the indications regarding security relevant gaps that could develop and we treat those seriously.

If you think you have detected a security gap in one of our products, please send us an email to the following address:

vulnerabilities@avira.com

9. Reference: Configuration options

The configuration reference documents all available configuration options.

9.1 System Scanner

You can define the behavior of the on-demand scan routine. If you select certain directories to be scanned, depending on the configuration, the System Scanner scans:

- with a certain scanning priority,
- also boot sectors and main memory,
- all or selected files in the directory.

Files

The System Scanner can use a filter to scan only those files with a certain extension (type).

All files

If this option is enabled, all files are scanned for viruses or unwanted programs, irrespective of their content and file extension. The filter is not used.

> **Note**
> If **All files** is enabled, the button **File extensions** cannot be selected.

Use smart extensions

If this option is enabled, the selection of the files scanned for viruses or unwanted programs is automatically chosen by the program. This means that your Avira program decides whether the files are scanned or not based on their content. This procedure is somewhat slower than Use file extension list, but more secure, since not only on the basis of the file extension is scanned. This option is enabled as the default setting and is recommended.

> **Note**
> If **Use smart extensions** is enabled, the button **File extensions** cannot be selected.

Use file extension list

If this option is enabled, only files with a specified extension are scanned. All file types that may contain viruses and unwanted programs are preset. The list can be edited manually via the button "**File extension**".

Note
If this option is enabled and you have deleted all entries from the list with file extensions, this is indicated with the text "*No file extensions*" under the button **File extensions**.

File extensions

With the aid of this button, a dialog box is opened in which all file extensions are displayed that are scanned in "**Use file extension list"** mode. Default entries are set for the extensions, but entries can be added or deleted.

Note
Please note that the default list may vary from version to version.

Additional settings

Scan boot sectors of selected drives

If this option is enabled, the System Scanner scans the boot sectors of the drives selected for the system scan. This option is enabled as the default setting.

Scan master boot sectors

If this option is enabled, the System Scanner scans the master boot sectors of the hard disk(s) used in the system.

Ignore offline files

If this option is enabled, the direct scan ignores so-called offline files completely during a scan. This means that these files are not scanned for viruses and unwanted programs. Offline files are files that were physically moved by a so-called Hierarchical Storage Management System (HSMS) from the hard disk onto a tape, for example. This option is enabled as the default setting.

Optimized scan

When the option is enabled, the processor capacity is optimally utilized during a System Scanner scan. For performance reasons, an optimized scan is only logged on standard level.

Note
This option is only available on multi-processor systems, but is always displayed in the configuration and can be enabled: If the managed server does not have more than one processor, the System Scanner option is not used.

Follow symbolic links

If this option is enabled, System Scanner performs a scan that follows all symbolic links in the scan profile or selected directory and scans the linked files for viruses and malware.

Note
The option does not include any shortcuts, but refers exclusively to symbolic links (generated by mklink.exe) or Junction Points (generated by junction.exe) that are transparent in the file system.

Note
The rootkits scan is not available for Windows XP 64 bit, Windows 2003 64 bit or Windows Server 2003 64 bit!

Note
The rootkit scan is not performed remotely.

Scan Registry

If this option is enabled, the Registry is scanned for references to malware. This option only changes the settings of profiles created by you.

Scan process

Scanner priority

With the on-demand scan, the System Scanner distinguishes between priority levels. This is only effective if several processes are running simultaneously on the workstation. The selection affects the scanning speed.

low

The System Scanner is only allocated processor time by the operating system, if no other process requires computation time, i.e. as long as only the System Scanner is running, the speed is maximum. All in all, work with other programs is optimal: The computer responds more quickly if other programs require computation time while the System Scanner continues running in the background.

normal

The System Scanner is executed with normal priority. All processes are allocated the same amount of processor time by the operating system. This option is enabled as the default setting and is recommended. Under certain circumstances, work with other applications may be affected.

high

The System Scanner has the highest priority. Simultaneous work with other applications is almost impossible. However, the System Scanner completes its scan at maximum speed.

9.1.1 Action on detection

You can define the actions to be performed by System Scanner when a virus or unwanted program is detected.

Copy file to quarantine before action

If this option is enabled, the System Scanner creates a backup copy before carrying out the requested primary or secondary action. The back-up copy is saved in Quarantine, where the file can be restored if it is of informative value. You can also send the backup copy to the Avira Malware Research Center for further investigation.

Primary action

Primary action is the action performed when the System Scanner finds a virus or an unwanted program. If the option "**Repair"** is selected but the affected file cannot be repaired, the action selected under "**Secondary action"** is performed.

> **Note**
> The option **Secondary action** can only be selected if the setting **Repair** was selected under **Primary action**.

Repair

If this option is enabled, the System Scanner repairs affected files automatically. If the System Scanner cannot repair an affected file, it carries out the action selected under Secondary action.

> **Note**
> An automatic repair is recommended, but means that the System Scanner modifies files on the workstation.

Rename

If this option is enabled, the System Scanner renames the file. Direct access to these files (e.g. with double-click) is therefore no longer possible. Files can later be repaired and given their original names again.

Quarantine

If this option is enabled, the System Scanner moves the file to the quarantine. These files can later be repaired or - if necessary - sent to the Avira Malware Research Center.

Delete

If this option is enabled, the file is deleted. This process is much faster than "overwrite and delete".

Ignore

If this option is enabled, access to the file is allowed and the file is left as it is.

Warning
The affected file remains active on your workstation! It may cause serious damage on your workstation!

Overwrite and delete

If this option is enabled, the System Scanner overwrites the file with a default pattern and then deletes it. It cannot be restored.

Secondary action

The option "**Secondary action"** can only be selected if the setting **Repair** was selected under "**Primary action"**. With this option it can now be decided what is to be done with the affected file if it cannot be repaired.

Rename

If this option is enabled, the System Scanner renames the file. Direct access to these files (e.g. with double-click) is therefore no longer possible. Files can later be repaired and given their original names again.

Quarantine

If this option is enabled, the System Scanner moves the file to Quarantine. These files can later be repaired or - if necessary - sent to the Avira Malware Research Center.

Delete

If this option is enabled, the file is deleted. This process is much faster than "overwrite and delete".

Ignore

If this option is enabled, access to the file is allowed and the file is left as it is.

Warning
The affected file remains active on your workstation! It may cause serious damage on your workstation!

Overwrite and delete

If this option is enabled, the System Scanner overwrites the file with a default pattern and then deletes (wipes) it. It cannot be restored.

Note
If you have selected **Delete** or **Overwrite and delete** as the primary or secondary action, you should note the following: In the case of heuristic hits, the affected files are not deleted, but are instead moved to quarantine.

9.1.2 Further actions

Launch program following detection

After the on-demand scan, the System Scanner can open a file of your choice if at least one virus or unwanted program has been detected, for example an email program, so that you can inform other users or the administrator.

Note
For security reasons it is only possible to start a program after a detection when a user is logged on the computer. The file is then opened with the rights that apply to the logged on user. If no user is logged on, this option is not performed.

Program name

In this input box you can enter the name and the relevant path of the program that the System Scanner should start after a detection.

This button opens a window in which you can select the desired program with the aid of the file selection dialog.

Arguments

In this input box you can enter command line parameters for the program to be started if necessary.

Event log

Use event log

If this option is enabled, an event report with the results of the scan is transferred to the Windows Event Log after a System Scanner scan has been completed. The events can be called up in the Windows Event Viewer. The option is disabled as the default setting.

9.1.3 Archives

When scanning archives, the System Scanner uses a recursive scan: Archives in archives are also unpacked and scanned for viruses and unwanted programs. The files are scanned, decompressed and scanned again.

Scan archives

If this option is enabled, the selected archives in the archive list are scanned. This option is enabled as the default setting.

All archive types

If this option is enabled, all archive types in the archive list are selected and scanned.

Smart Extensions

If this option is enabled, the System Scanner detects whether a file is a packed file format (archive), even if the file extension differs from the usual extensions, and scans the archive. However every file must be opened for this, which reduces the scanning speed. Example: If a *.zip archive has the file extension *.xyz, the System Scanner also unpacks this archive and scans it. This option is enabled as the default setting.

> **Note**
> Only those archive types marked in the archive list are supported.

Limit recursion depth

Unpacking and scanning recursive archives can require a great deal of computer time and resources. If this option is enabled, you limit the depth of the scan in multi-packed archives to a certain number of packing levels (maximum recursion depth). This saves time and computer resources.

> **Note**
> In order to find a virus or an unwanted program in an archive, the System Scanner must scan up to the recursion level in which the virus or the unwanted program is located.

Maximum recursion depth

In order to enter the maximum recursion depth, the option Limit recursion depth must be enabled.
You can either enter the requested recursion depth directly or by means of the right arrow key on the entry field. The permitted values are 1 to 99. The standard value is 20 which is recommended.

Default values

The button restores the pre-defined values for scanning archives.

Archives

In this display area you can set which archives the System Scanner should scan. For this, you must select the relevant entries.

9.1.4 Exceptions

File objects to be omitted for the System Scanner

The list in this window contains files and paths that should not be included by the System Scanner in the scan for viruses or unwanted programs.

Please enter as few exceptions as possible here and really only files that, for whatever reason, should not be included in a normal scan. We recommend that you always scan these files for viruses or unwanted programs before they are included in this list!

Note
The entries in the list must not result in more than 6000 characters in total.

Warning
These files are not included in a scan!

Note
The files included in this list are recorded in the report file. Please check the report file from time to time for unscanned files, as perhaps the reason you excluded a file here no longer exists. In this case you should remove the name of this file from this list again.

Input box

In this input box you can enter the name of the file object that is not included in the on-demand scan. No file object is entered as the default setting.

The button opens a window in which you can select the required file or the required path.
When you have entered a file name with its complete path, only this file is not scanned for infection. If you have entered a file name without a path, all files with this name (irrespective of the path or drive) are not scanned.

Add

With this button, you can add the file object entered in the input box to the display window.

Delete

The button deletes a selected entry from the list. This button is inactive if no entry is selected.

Note
If you are managing the Avira program in AMC, you can use variables in the path details for file exceptions. You can find a list of variables you can use under Variables: Real-Time Protection und System Scanner Exceptions.

9.1.5 Heuristic

This configuration section contains the settings for the heuristic of the scan engine.

Avira products contain very powerful heuristics that can proactively uncover unknown malware, i.e. before a special virus signature to combat the damaging element has been created and before a virus guard update has been sent. Virus detection involves an extensive analysis and investigation of the affected codes for functions typical of malware. If the code being scanned exhibits these characteristic features, it is reported as being suspicious. This does not necessarily mean that the code is in fact malware. False positives do sometimes occur. The decision on how to handle affected code is to be made by the user, e.g. based on his or her knowledge of whether the source of the code is trustworthy or not.

Macrovirus heuristic

Macrovirus heuristic

Your Avira product contains a highly powerful macrovirus heuristic. If this option is enabled, all macros in the relevant document are deleted in the event of a repair, alternatively suspect documents are only reported, i.e. you receive an alert. This option is enabled as the default setting and is recommended.

Advanced Heuristic Analysis and Detection (AHeAD)

Enable AHeAD

Your Avira program contains a very powerful heuristic in the form of Avira AHeAD technology, which can also detect unknown (new) malware. If this option is enabled, you can define how "aggressive" this heuristic should be. This option is enabled as the default setting.

Low detection level

If this option is enabled, slightly less unknown malware is detected, the risk of false alerts is low in this case.

Medium detection level

This option combines a strong detection level with a low risk of false alerts. Medium is the default setting if you have selected the use of this heuristic.

High detection level

If this option is enabled, significantly more unknown malware is detected, but there are also likely to be false positives.

9.1.6 Report

The System Scanner has a comprehensive reporting function. You thus obtain precise information on the results of an on-demand scan. The report file contains all entries of the system as well as alerts and messages of the on-demand scan.

> **Note**
> To be able to establish what actions the System Scanner has performed, when viruses or unwanted programs have been detected, you should activate the report file in the expert-mode configuration.

Reporting

Off

If this option is enabled, the System Scanner does not report the actions and results of the on-demand scan.

Default

When this option is activated, the System Scanner logs the path and names of the concerning files. In addition, the configuration for the current scan, version information and information on the licensee is written in the report file.

Extended

When this option is activated, the System Scanner logs alerts and tips in addition to the default information.

Complete

When this option is activated, the System Scanner also logs all scanned files. In addition, all files involved as well as alerts and tips are included in the report file.

> **Note**
> If you have to send us a report file at any time (for troubleshooting), please create this report file in this mode.

9.2 Real-Time Protection

You will normally want to monitor your system constantly. To this end, use the Real-Time Protection (= on-access System Scanner). You can thus scan all files that are copied or opened on the computer "on the fly", for viruses and unwanted programs.

Files

The Real-Time Protection can use a filter to scan only those files with a certain extension (type).

All files

If this option is enabled, all files are scanned for viruses or unwanted programs, irrespective of their content and their file extension.

> **Note**
> If **All files** is enabled, the **File extensions** button cannot be selected.

Use smart extensions

If this option is enabled, the selection of the files scanned for viruses or unwanted programs is automatically chosen by the program. This means that the program decides whether the files are scanned or not based on their content. This procedure is somewhat slower than **Use file extension list**, but more secure, since not only on the basis of the file extension is scanned.

> **Note**
> If **Use smart extensions** is enabled, the **File extensions** button cannot be selected.

Use file extension list

If this option is enabled, only files with a specified extension are scanned. All file types that may contain viruses and unwanted programs are preset. The list can be edited manually via the "**File extensions"** button. This option is enabled as the default setting and is recommended.

> **Note**
> If this option is enabled and you have deleted all entries from the list with file extensions, this is indicated with the text "No file extensions" under the **File extensions** button.

File extensions

With the aid of this button, a dialog box is opened in which all file extensions are displayed that are scanned in "**Use file extension list"** mode. Default entries are set for the extensions, but entries can be added or deleted.

> **Note**
> Please note that the file extension list may vary from version to version.

Scan mode

Here the time for scanning of a file is defined.

Scan when reading

If this option is enabled, the Real-Time Protection scans the files before they are read or executed by the application or the operating system.

Scan when writing

If this option is enabled, the Real-Time Protection scans a file when writing. You can only access the file again after this process has been completed.

Scan when reading and writing

If this option is enabled, the Real-Time Protection scans files before opening, reading and executing and after writing. This option is enabled as the default setting and is recommended.

Drives

Monitor local drives

When the option has been activated, files of local drives, such as HDUs, CD and diskette drives, MO and ZIP drives, etc. only are monitored. This option is enabled as the default setting and is recommended.

Monitor network drives

If this option is enabled, files on network drives (mapped drives) such as server volumes, peer drives etc., are scanned.

Note
In order not to reduce the performance of your computer too much, the option **Monitor network drives** should only be enabled in exceptional cases.

Warning
If this option is disabled, the network drives are **not** monitored. They are no longer protected against viruses or unwanted programs!

Note
When files are executed on network drives, they are scanned by the Real-Time Protection irrespective of the setting for the **Monitor network drives** option. In some cases files on network drives are scanned while being opened, even though the **Monitor network drives** option is disabled. Reason: These files are accessed with ‘Execute File’ rights. If you want to exclude these files or even executed files on network drives from scanning by the Real-Time Protection,

enter the files in the list of file objects to be excluded (see: Real-Time Protection > Scan > Exceptions).

Enable caching

If this option is enabled, monitored files on network drives will be made available in the Real-Time Protection's cache. Monitoring of network drives without the caching function is more secure, but does not perform as well as the monitoring of network drives with caching.

Archives

Scan archives

If this option is enabled, then archives will be scanned. Compressed files are scanned, then decompressed and scanned again. This option is deactivated by default. The archive scan is restricted by the recursion depth, the number of files to be scanned and the archive size. You can set the maximum recursion depth, the number of files to be scanned and the maximum archive size.

Note
This option is deactivated by default, since the process puts heavy demands on the computer's performance. It is generally recommended that archives be checked using an on-demand scan.

Max. recursion depth

When scanning archives, the Real-Time Protection uses a recursive scan: Archives in archives are also unpacked and scanned for viruses and unwanted programs. You can define the recursion depth. The default value for the recursion depth is 1 and is recommended: all files that are directly located in the main archive are scanned.

Max. number of files

When scanning archives, you can restrict the scan to a maximum number of files in the archive. The default value for the maximum number of files to be scanned is 10 and is recommended.

Max. size (KB)

When scanning archives, you can restrict the scan to a maximum archive size to be unpacked. The standard value of 1000 KB is recommended.

9.2.1 Action on detection

You can define the actions to be performed by Real-Time Protection when a virus or unwanted program is detected. (Options available in expert mode only.)

Enhanced Terminal Server support

If this option is enabled, a dialog box appears, if a virus or unwanted program is detected during the on-access scan, in which you can choose what is to be done with the concerning file.

Permitted actions

In this display box you can specify the virus management actions that should be available as further actions in the dialog box. You must activate the corresponding options for this.

Repair

Real-Time Protection repairs the infected file if possible.

Rename

Real-Time Protection renames the file. Direct access to these files (e.g. with double-click) is therefore no longer possible. The file can be repaired at a later time and renamed again.

Quarantine

Real-Time Protection moves the file to Quarantine. The file can be recovered from Quarantine manager if it has an informative value or - if necessary - sent to the Avira Malware Research Center. Depending on the file, further options are available in the Quarantine manager.

Delete

The file will be deleted. This process is much faster than **Overwrite and delete** (see below).

Ignore

Access to the file is permitted and the file is ignored.

Overwrite and delete

Real-Time Protection overwrites the file with a default pattern before deleting it. It cannot be restored.

Deny access

Access is denied to the file. Real-Time Protection logs the detection in the report file, if the Report function is enabled. Real-Time Protection also appends an entry to the Windows Event log, if this option is enabled.

Warning
If Real-Time Protection is set to **Scan when writing**, the affected file is not written.

Default

This button allows you to select an action that is activated in the dialog box by default when a virus is detected. Select the action that should be activated by default and click on the "**Default**" button.

> **Note**
> The action **Repair** cannot be selected as the default action.

Click here for more information.

Automatic

If this option is enabled, no dialog box in case of a virus detection appears. Real-Time Protection reacts according to the settings you predefine in this section as primary and secondary action.

Copy file to quarantine before action

If this option is enabled, the Real-Time Protection creates a backup copy before carrying out the requested primary or secondary action. The backup copy is saved in quarantine. It can be restored via the Quarantine manager if it is of informative value. You can also send the backup copy to the Avira Malware Research Center. Depending on the object, more selection options are available in the Quarantine manager.

Primary action

Primary action is the action performed when the Real-Time Protection finds a virus or an unwanted program. If the "**Repair**" option is selected but the affected file cannot be repaired, the action selected under "**Secondary action**" is performed.

> **Note**
> The **Secondary action** option can only be selected if the **Repair** setting was selected under **Primary action**.

Repair

If this option is enabled, the Real-Time Protection repairs affected files automatically. If the Real-Time Protection cannot repair an affected file, it carries out the action selected under **Secondary action**.

> **Note**
> An automatic repair is recommended, but means that the Real-Time Protection modifies files on the workstation.

Rename

If this option is enabled, the Real-Time Protection renames the file. Direct access to these files (e.g. with double-click) is therefore no longer possible. Files can later be repaired and given their original names again.

Quarantine

If this option is enabled, the Real-Time Protection moves the file to Quarantine. The files in this directory can later be repaired or - if necessary - sent to the Avira Malware Research Center.

Delete

If this option is enabled, the file is deleted. This process is much faster than **Overwrite and delete**.

Ignore

If this option is enabled, access to the file is allowed and the file is left as it is.

Warning
The affected file remains active on your workstation! It may cause serious damage on your workstation!

Overwrite and delete

If this option is enabled, the Real-Time Protection overwrites the file with a default pattern and then deletes it. It cannot be restored.

Deny access

If this option is enabled, the Real-Time Protection only enters the detection in the report file if the report function is enabled. In addition, the Real-Time Protection writes an entry in the Event log, if this option is enabled.

Warning
If Real-Time Protection is set to **Scan when writing**, the affected file is not written.

Secondary action

The option **Secondary action** can only be selected if the **Repair** option was selected under **Primary action**. With this option it can now be decided what is to be done with the affected file if it cannot be repaired.

Rename

If this option is enabled, the Real-Time Protection renames the file. Direct access to these files (e.g. with double-click) is therefore no longer possible. Files can later be repaired and given their original names again.

Quarantine

If this option is enabled, the Real-Time Protection moves the file to Quarantine. The files can later be repaired or - if necessary - sent to the Avira Malware Research Center.

Delete

If this option is enabled, the file is deleted. This process is much faster than **Overwrite and delete**.

Ignore

If this option is enabled, access to the file is allowed and the file is left as it is.

Warning
The affected file remains active on your workstation! It may cause serious damage on your workstation!

Overwrite and delete

If this option is enabled, the Real-Time Protection overwrites the file with a default pattern and then deletes it. It cannot be restored.

Deny access

If this option is enabled, the affected file is not written; the Real-Time Protection only enters the detection in the report file if the report function is enabled. In addition, the Real-Time Protection writes an entry in the Event log, if this option is enabled.

Note
If you have selected **Delete** or **Overwrite and delete** as the primary or secondary action, please note: In the case of heuristic hits, the affected files are not deleted, but are instead moved to quarantine.

9.2.2 Further actions

Use event log

If this option is enabled, an entry is added to the Windows event log for every detection. The events can be called up in the Windows event viewer. This option is enabled as the default setting.

9.2.3 Exceptions

With these options you can configure exception objects for the Real-Time Protection (on-access scan). The relevant objects are then not included in the on-access scan. The Real-Time Protection can ignore file accesses to these objects during the on-access scan via the list of processes to be omitted. This is useful, for example, with databases or backup solutions.

Please note the following when specifying processes and file objects to be omitted: The list is processed from top to bottom. The longer the list is, the more processor time is required for processing the list for each access. Therefore, keep the list as short as possible.

Processes to be omitted by the Real-Time Protection

All file accesses of processes in this list are excluded from monitoring by Real-Time Protection.

Input box

In this field, enter the name of the process that is to be ignored by the real-time scan. No process is entered as the default setting.

The specified path and file name of the process should contain a maximum of 255 characters. You can enter up to 128 processes. The entries in the list must not result in more than 6000 characters in total.

When entering the process, Unicode symbols are accepted. You can therefore enter process or directory names containing special symbols.

Drive information must be entered as follows: `[Drive letter]:\`

The colon symbol (:) is only used to specify drives.

When specifying the process, you can use the wildcards * (any number of characters) and ? (a single character).

```
C:\Program Files\Application\application.exe
C:\Program Files\Application\applicatio?.exe
C:\Program Files\Application\applic*.exe
C:\Program Files\Application\*.exe
```

To avoid the process being excluded globally from monitoring by Real-Time Protection, specifications exclusively comprising the following characters are invalid: * (asterisk), ? (question mark), / (forward slash), \ (backslash), . (dot), : (colon).

You have the option of excluding processes from monitoring by the Real-Time Protection without full path details. For example: `application.exe`

This however only applies to processes where the executable files are located on hard disk drives.

Full path details are required for processes where the executable files are located on connected drives, e.g. network drives. Please note the general information on the notation of Exceptions on connected network drives.

Do not specify any exceptions for processes where the executable files are located on dynamic drives. Dynamic drives are used for removable disks, such as CDs, DVDs or USB sticks.

Warning
Please note that all file accesses done by processes recorded in the list are excluded from the scan for viruses and unwanted programs!

The button opens a window in which you can select an executable file.

Add

With this button, you can add the process entered in the input box to the display window.

Delete

With this button you can delete a selected process from the display window.

File objects to be omitted by the Real-Time Protection

All file accesses to objects in this list are excluded from monitoring by the Real-Time Protection.

Input box

In this box you can enter the name of the file object that is not included in the on-access scan. No file object is entered as the default setting.

The entries in the list must have no more than 6000 characters in total.

When specifying file objects to be omitted, you can use the wildcards* (any number of characters) and ? (a single character): Individual file extensions can also be excluded (including wildcards):

```
C:\Directory\*.mdb
*.mdb
*.md?
*.xls*
C:\Directory\*.log
```

Directory names must end with a backslash \ .

If a directory is excluded, all its sub-directories are automatically also excluded.

For each drive you can specify a maximum of 20 exceptions by entering the complete path (starting with the drive letter). For example:

```
C:\Program Files\Application\Name.log
```

The maximum number of exceptions without a complete path is 64. For example:

```
*.log
\computer1\C\directory1
```

In case of dynamic drives that are mounted as a directory on another drive, the alias of the operating system for the integrated drive in the list of the exceptions has to be used, e.g.:

`\Device\HarddiskDmVolumes\PhysicalDmVolumes\BlockVolume1\`

If you use the mount point itself, for example, `C:\DynDrive`, the dynamic drive will be scanned nonetheless. You can determine the alias of the operating system to be used from the Real-Time Protection report file.

The button opens a window in which you can select the file object to be excluded.

Add

With this button, you can add the file object entered in the input box to the display window.

Delete

With this button you can delete a selected file object from the display window.

Please note the further information when specifying exceptions:

In order to also exclude objects when they are accessed with short DOS file names (DOS name convention 8.3), the relevant short file name must also be entered in the list.

A file name that contains wildcards may not be terminated with a backslash. For example:
`C:\Program Files\Application\applic*.exe\`
This entry is not valid and not treated as an exception!

Please note the following with regard to **exceptions on connected network drives**: If you use the drive letter of the connected network drive, the files and folders specified are NOT excluded from the Real-Time Protection scan. If the UNC path in the list of exceptions differs from the UNC path used to connect to the network drive (IP address specification in the list of exceptions – specification of computer name for connection to network drive), the specified folders and files are NOT excluded by the Real-Time Protection scan. Locate the relevant UNC path in the Real-Time Protection report file:
`\\<Computer name>\<Enable>\` - OR - `\\<IP address>\<Enable>\`

You can locate the path Real-Time Protection uses to scan for infected files in the Real-Time Protection report file. Indicate exactly the same path in the list of exceptions. Proceed as follows: Set the protocol function of the Real-Time Protection to **Complete** in the configuration under Real-Time Protection > Report. Now access the files, folders, mounted drives or connected network drives with the activated Real-Time Protection. You can now read the path to be used from the Real-Time Protection report file.

If you are managing the Avira product in AMC, you can use variables in the path details for process and file exceptions. You can find a list of variables you can use under Variables: Real-Time Protection and Scanner Exceptions.

Examples for processes to be excluded:

- `application.exe`
  The *application.exe* process is excluded from the Real-Time Protection scan, irrespective of which hard disk drive it is located on and which directory it is in.
- `C:\Program Files1\Application.exe`
  The process for the file *application.exe*, which is located under the path *C:\Program Files1*, is excluded from the Real-Time Protection scan.
- `C:\Program Files1\*.exe`
  All processes for executable files located under the path *C:\Program Files1* are excluded from the Real-Time Protection scan.

Examples for files to be excluded:

- `*.mdb`
  All files with the extension '*mdb*' are excluded from the Real-Time Protection scan.
- `*.xls*`
  All files with a file extension beginning '*xls*' are excluded from the Real-Time Protection scan, e.g. files with the extensions *.xls* and *.xlsx*.
- `C:\Directory\*.log`
  All log files with the extension '*log*', located under the path *C:\Directory*, are excluded from the Real-Time Protection scan.
- `\\Computer name\Shared1\`
  All files are excluded from the Real-Time Protection scan accessed via a connection '*Computer name1**Shared1*'. This is generally a connected network drive which accesses another computer with a shared folder via the computer name '*Computer name1*' and the shared name '*Shared1*'.
- `\\1.0.0.0\Shared1\*.mdb`
  All files with the extension '*mdb*' are excluded from the Real-Time Protection scan accessed via a connection '*1.0.0.0**Shared1*'. This is generally a connected network drive which accesses another computer with a shared folder via the IP address '1.0.0.0' and the shared name '*Shared1*'.

9.2.4 Products

Products to be skipped by Real-Time Protection

In this display box, you can select products which are excluded by the Realtime Protection scan. All applications, services or databases of the selected product are excluded from the monitoring by Real-Time Protection.

9.2.5 Heuristic

This configuration section contains the settings for the heuristic of the scan engine.

Avira products contain very powerful heuristics that can proactively uncover unknown malware, i.e. before a special virus signature to combat the damaging element has been created and before a virus guard update has been sent. Virus detection involves an extensive analysis and investigation of the affected codes for functions typical of malware. If the code being scanned exhibits these characteristic features, it is reported as being suspicious. This does not necessarily mean that the code is in fact malware. False positives do sometimes occur. The decision on how to handle affected code is to be made by the user, e.g. based on his or her knowledge of whether the source of the code is trustworthy or not.

Macrovirus heuristics

Macrovirus heuristics

Your Avira product contains a highly powerful macrovirus heuristic. If this option is enabled, all macros in the relevant document are deleted in the event of a repair, alternatively suspect documents are only reported, i.e. you receive an alert. This option is enabled as the default setting and is recommended.

Advanced Heuristic Analysis and Detection (AHeAD)

Enable AHeAD

Your Avira program contains a very powerful heuristic in the form of Avira AHeAD technology, which can also detect unknown (new) malware. If this option is enabled, you can define how "aggressive" this heuristic should be. This option is enabled as the default setting.

Low detection level

If this option is enabled, slightly less unknown malware is detected, the risk of false alerts is low in this case.

Medium detection level

This option combines a strong detection level with a low risk of false alerts. Medium is the default setting if you have selected the use of this heuristic.

High detection level

If this option is enabled, significantly more unknown malware is detected, but there are also likely to be false positives.

9.2.6 Report

Real-Time Protection includes an extensive logging function to provide the user or administrator with exact notes about the type and manner of a detection.

Reporting

This group allows for the content of the report file to be determined.

Off

If this option is enabled, then Real-Time Protection does not create a log.
It is recommended that you should turn off the logging function only in exceptional cases, such as if you are executing trials with multiple viruses or unwanted programs.

Default

If this option is enabled, Real-Time Protection records important information (concerning detections, alerts and errors) in the report file, with less important information ignored for improved clarity. This option is enabled as the default setting.

Extended

If this option is enabled, Real-Time Protection logs less important information to the report file as well.

Complete

If this option is enabled, Real-Time Protection logs all available information in the report file, including file size, file type, date, etc.

Limit report file

Limit size to n MB

If this option is enabled, the report file can be limited to a certain size. Permitted values are between 1 and 100 MB. Around 50 kilobytes of extra space are allowed when limiting the size of the report file to minimize the use of system resources. If the size of the log file exceeds the indicated size by more than 50 kilobytes, then old entries are deleted until the indicated size minus 50 kilobytes is reached.

Back up report file before shortening

If this option is enabled, the report file is backed up before shortening. For the save location see Report directory.

Write configuration to report file

If this option is enabled, the configuration of the on-access scan is recorded in the report file.

Note
If you have not specified any report file restriction, a new report file is automatically created when the report file reaches 100MB. A backup of the old report file is created. Up to three backups of old report files are saved. The oldest backups are deleted first.

9.3 Variables: Real-Time Protection and System Scanner exceptions

If your Avira product is managed with AMC, you may use variables to configure exceptions for the Real-Time Protection and the System Scanner. When saving the configuration on the managed system, the variables are automatically replaced by true values corresponding to the operating system and its language.

The following variables may be used:

9.3.1 Variables for Windows XP 32-Bit (**English)

Variable	Windows XP 32-Bit (**English)
%WINDIR%	*C:\Windows*
%SYSDIR%	*C:\Windows\System32*
%ALLUSERSPROFILE%	*C:\Documents and Settings\All Users* **
%PROGRAMFILES%	*C:\Program Files* **
%PROGRAMFILES(x86)%	%PROGRAMFILES(x86)%
%SYSTEMROOT%	*C:\Windows*
%INSTALLDIR%	*C:\Program Files\Avira\Antivir Desktop* **
%AVAPPDATA%	*C:\Documents and Settings\All Users\Avira\AntiVir Desktop* **

The paths marked with **** are language dependent. The above mentioned examples name the relevant paths on an English operating system.

9.3.2 Variables for Windows 7 32-Bit/ 64-Bit (**English)

Variable	Windows 7 32-Bit (**English)	Windows 7 64-Bit (**English)
%WINDIR%	*C:\Windows*	*C:\Windows*
%SYSDIR%	*C:\Windows\System32*	*C:\Windows\System32*
%ALLUSERSPROFILE%	*C:\ProgramData*	*C:\ProgramData*
%PROGRAMFILES%	*C:\Program Files* **	*C:\Program Files* **
%PROGRAMFILES(x86)%	%PROGRAMFILES(x86)%	*C:\Program Files (x86)* **
%SYSTEMROOT%	*C:\Windows*	*C:\Windows*
%INSTALLDIR%	*C:\Program Files\Avira\Antivir Desktop* **	*C:\Program Files (x86)\Avira\Antivir Desktop* **
%AVAPPDATA%	*C:\ProgramData\Avira\AntiVir Desktop*	*C:\ProgramData\Avira\AntiVir Desktop*

The paths marked with **** are language dependent. The above mentioned examples name the relevant paths on an English operating system.

9.4 Update

The connection to the download servers is configured in the **Update** section.

Download

via web server

The update is performed via a web server using an HTTP connection. You can use a proprietary web server on the Internet or a web server on an intranet, which obtains the update files from a proprietary download server on the Internet.

Note
You can access further settings for updating via a web server under: Configuration > Local protection > Update > Web server.

If this option is enabled, you can configure the Web server and, where necessary, the proxy server.

via file server / shared folders

The update is performed via a file server on an intranet which obtains the update files from a proprietary download server on the Internet.

Note
You can access further settings for updating via a file server under: Configuration > Local protection > Update > File server.
If this option is enabled, you can configure the file server you are using.

9.4.1 Product update

Under **Product update**, configure how product updates or the notification of available product updates are handled.

Product updates

Download and install product updates automatically

When this option is enabled, you can define a time for the product update. Specify a day and time for the product update. The product update will take place at this time, provided there are product updates available. Updates to the virus definition file and scan engine are performed independently of this setting. The conditions for this option are: complete configuration of the update and an open connection to a download server. Before a product update is performed, you will receive an alert on the Avira Server Security Console used to manage the server to be protected.

Download product updates. If a restart is necessary, install the update after the system restart, otherwise install it immediately

If this option is enabled, product updates will be downloaded as soon as they become available. If no restart is necessary, the update is installed automatically after the update file is downloaded. If a product update requires you to restart your computer, it will be executed at the next user-controlled system reboot and not immediately after the download of the update file. This has the advantage that the restart is not performed while users are working at their computers. Updates to the virus definition file and scan engine are performed independently of this setting. The conditions for this option are: complete configuration of the update and an open connection to a download server.

Notify user if product updates are available

If this option is enabled, you will only be notified when new product updates become available. Updates to the virus definition file and scan engine are performed independently of this setting. The conditions for this option are: complete configuration

of the update and an open connection to a download server. You will be notified in the Avira Server Security Console and by email, if email notification has been configured.

Notify once again after n day(s)

If the product update was not installed after the initial notification, enter in this box the number of days that are to elapse before you are again notified that product updates are available.

> **Warning**
> An update of the virus definition file and of the search engine is performed during every update process independent of the settings for the product update (see Chapter Updates).

9.4.2 Web server

The update can be performed directly via a web server on the Internet or the intranet.

Download

Priority server

In this field, enter the update directory and URL of the web server that will first be requested to provide the update. If this server cannot be reached, the standard servers indicated will be used. The format for the address of the web server is as follows: `http://<hostname or IP>[:port]/update`. If you do not specify a port, port 80 will be used.

Default server

Enter the URL and update directory of the web servers from which the updates are to be downloaded. Multiple entries are separated by commas. The address format is: `http://<hostname or IP>[:port]/update`. If you do not specify a port, port 80 will be used. By default, the accessible Avira web servers are specified for updating. You can, however, use your own web servers on the company intranet. If a number of web servers are specified, separate each one by a comma.

Default

The button restores the predefined addresses.

9.4.3 Proxy settings

Proxy server

Do not use a proxy server

If this option is enabled, your connection to the web server is not established via a proxy server.

Warning
If you are using a proxy server which requires authentication, enter all the required data under the option **Use this proxy server**. The **Use proxy system settings** option can only be used for proxy servers without authentication.

Use this proxy server

If your web server connection is set up via a proxy server, you can enter the relevant information here.

Address

Enter the computer name or IP address of the proxy server you want to use to connect to the web server.

Port

Please enter the port number of the proxy server you want to use to connect to the web server.

Login name

Enter a user name to log in on the proxy server.

Login password

Enter the relevant password for logging in on the proxy server here. For security reasons, the actual characters you type in this space are replaced by asterisks (*).

Examples:

Address: `proxy.domain.com` Port: `8080`

Address: `192.168.1.100` Port: `3128`

9.5 General

9.5.1 Threat categories

Selection of extended threat categories

Your Avira product protects you against computer viruses. In addition, you can scan according to the following extended threat categories.

- Adware
- Adware/Spyware
- Applications
- Backdoor Clients
- Dialer
- Double Extension Files

- Fraudulent software
- Games
- Jokes
- Phishing
- Programs that violate the private domain
- Unusual runtime packers

By clicking on the relevant box, the selected type is enabled (check mark set) or disabled (no check mark).

Select all

If this option is enabled, all types are enabled.

Default values

This button restores the predefined default values.

> **Note**
> If a type is disabled, files recognized as being of the relevant program type are no longer indicated. No entry is made in the report file.

9.5.2 Password

You can restrict the access to servers you wish to protect in the Avira Server Security Console with a password. The password of the server must always be entered when a connection is made to the server. Connection to servers protected by a password is ended as soon as you close the Avira Server Security Console.

Password

Enter password

Enter your required password here. For security reasons, the actual characters you type in this space are replaced by asterisks (*). The password can only have a maximum of 20 chars. Once the password has been issued, the program refuses access if an incorrect password is entered. An empty box means "No password".

Confirmation

Confirm the password entered above by entering again here. For security reasons, the actual characters you type in this space are replaced by asterisks (*).

> **Note**
> The password is case-sensitive!

9.5.3 WMI

Support for Windows Management Instrumentation

Windows Management Instrumentation is a basic Windows management technology that uses script and programming languages to allow read and write access, both local and remote, to settings on Windows systems. Your Avira product supports WMI and provides data (status information, statistical data, reports, planned requests, etc.) as well as events and methods (stopping and starting processes) via an interface. WMI gives you the option of downloading operating data from the program and controlling the program. You can request a complete reference guide to the WMI interface from the manufacturer. The reference file is available in PDF format when you sign a confidentiality agreement.

Enable WMI support

When this option is enabled, you can download operating data from the program via WMI.

Allow services to be enabled/disabled

When this option is enabled, you can enable and disable program services via WMI.

9.5.4 Events

Limit size of event database

Limit size to max. n entries

If this option is enabled, the maximum number of events listed in the event database can be limited to a certain size; possible values: 100 to 10000 entries. If the number of entered entries is exceeded, the oldest entries are deleted.

Delete all events older than n day(s)

If this option is enabled, events listed in the event database are deleted after a certain period of time; possible values: 1 to 90 days. This option is enabled as the default setting, with a value of 30 days.

No limit

When this option has been activated, the size of the event database is not limited. However, a maximum of 20,000 entries are displayed in the program interface under Events.

9.5.5 Reports

Limit reports

Limit number to max. n piece

When this option is enabled, the maximum number of reports can be limited to a specific amount. Values between 1 and 300 are permissible. If the specified number is exceeded, then the oldest report at that time is deleted.

Delete all reports older than n day(s)

If this option is enabled, reports are automatically deleted after a specific number of days. Permissible values are: 1 to 90 days. This option is enabled as the default setting, with a value of 30 days.

No limit

If this option is enabled, the number of reports is not restricted.

9.5.6 Directories

Temporary path

Use default system settings

If this option is enabled, the settings of the system are used for handling temporary files.

Use following directory

If this option is enabled, the path displayed in the input box is used.

Input box

In this input box, enter the path where the program will store its temporary files.

The button opens a window in which you can select the required temporary path.

Default

The button restores the pre-defined directory for the temporary path.

Report directory

Input box

This input box contains the absolute path to the report directory.

The button opens a window in which you can select the required directory.

Default

The button restores the pre-defined path to the report directory.

Quarantine directory

Input box

This box contains the path to the quarantine directory.

The button opens a window in which you can select the required directory.

Default

The button restores the predefined path to the quarantine directory.

9.6 Alerts

You can send individually configurable alerts from the System Scanner or from the Realtime Protection to any workstations in your network.

> **Note**
> An alert is always sent to computers, **not** to a certain user.

> **Warning**
> This functionality is **no longer supported** by the following operating systems:
> Windows Server 2008 and higher
> Windows Vista and higher

Send message to

The list in this window shows names of computers that receive a message when a virus or unwanted program is found.

> **Note**
> A computer can always be entered only once in this list.

Insert

With this button you can add a further computer. A window is opened in which you can enter the names of new computers. A computer name can be a maximum of 15 characters long.

The button opens a window in which you can alternatively select a computer directly from your computer environment.

Delete

With this button you can delete the currently selected entry from the list.

9.6.1 Real-Time Protection network alerts

Network alerts

If this option is enabled, network alerts are sent. This option is disabled as the default setting.

> **Note**
> To be able to activate this option, at least one recipient must be entered under Settings > Alerts > Network.

Message to be sent

The window shows the message sent to the selected workstation when a virus or unwanted program is detected. You can edit this message. A text may contain a maximum of 500 characters.

You can use the following key combinations for formatting the message:

Shortcut	Description
Ctrl + Tab	Inserts a tab The current line is indented by several characters to the right.
Ctrl + Enter	Inserts a line break

The message can include wildcards for information found during the search. These wildcards are replaced by the actual text when sent.

The following wildcards can be used:

Wildcard	Description
%VIRUS%	Contains the name of the detected virus or of the unwanted program
%FILE%	Contains the path and file name of the affected file
%COMPUTER%	Contains the name of the computer on which the Real-Time Protection is running
%NAME%	Contains the name of the user who accessed the affected file

%ACTION%	Contains the action performed after the detection of the virus
%MACADDR%	Contains the MAC address of the computer on which the Real-Time Protection is running

Default

The button restores the predefined default text for an alert.

9.6.2 System Scanner network alerts

Enable network alerts

If this option is enabled, network alerts are sent. This option is disabled as the default setting.

> **Note**
> To be able to activate this option, at least one recipient must be entered under Settings > Alerts > Network.

Message to be sent

The window shows the message sent to the selected workstation when a virus or unwanted program is detected. You can edit this message. A text may contain a maximum of 500 characters.

You can use the following key combinations for formatting the message:

Shortcuts	Description
Ctrl + Tab	Inserts a tab The current line is indented by several characters to the right
Ctrl + Enter	Inserts a line break

The message can include wildcards for information found during the search. These wildcards are replaced by the actual text when sent.

The following wildcards can be used:

Wildcard	Description
%VIRUS%	Contains the name of the detected virus or of the unwanted program
%NAME%	Contains the name of the logged in user using the System Scanner
%COMPUTER%	Contains the name of the computer on which the System Scanner is running

Default

The button restores the predefined default text for an alert.

9.6.3 Acoustic alerts

You can deactivate or activate an acoustic alert to signal that a virus has been found during a scan by the Real-Time Protection. The acoustic alert is only emitted in "*Extended terminal server support*" action mode. An alternative WAVE file can be selected as an acoustic alert.

> **Note**
> The action mode for the Real-Time Protection is set under the following heading:
> Settings > Real-Time Protection > Action on detection

No warning

When this option is activated, there is no acoustic alert when a virus is detected by the Real-Time Protection.

Use PC speakers (only in interactive mode)

When this option is activated, there is an acoustic alert with the default signal when a virus is detected by the Real-Time Protection. The acoustic alert is sounded on the PC's internal speaker.

Use the following WAVE file (only in interactive mode)

If this option is enabled, there is an acoustic alert with the selected WAV file when a virus is detected by the Real-Time Protection. The selected WAVE file is played over a connected external speaker.

WAVE file

In this input box you can enter the name and the associated path of an audio file of your choice. The program's default acoustic signal is entered as standard.

The button opens a window in which you can select the required file with the aid of the file explorer.

Test

This button is used to test the selected WAVE file.

9.7 Email

The Avira product can send alerts and messages via email to one or more recipients with certain events. This is done with the Simple Message Transfer Protocol (SMTP).

The messages can be triggered by various events. The following components support email sending:

- Real-Time Protection email alerts
- System Scanner email alerts
- Updater email alerts
- Quarantine manager: Sending suspicious files to the Avira Malware Research Center

> **Note**
> Please note that ESMTP is not supported. In addition, an encrypted transfer via TLS (Transport Layer Security) or SSL (Secure Sockets Layer) is currently not possible.

Email messages

SMTP Server

Enter the name of the host to be used here - either its IP address or the direct host name.
The maximum possible length of the host name is 127 characters.

For example*:*

`192.168.1.100` or `mail.samplecompany.com`.

Port

Enter the port to be used here.

Sender address

In this input box, enter the email address of the sender. The maximum length of the sender's address is 127 characters.

Authentication

Some mail servers expect a program to verify itself to the server (log in) before an email is sent. Alerts can be transmitted with authentication to an SMTP server via email.

Use authentication

If this option is enabled, a user name and a password can be entered in the relevant boxes for login (authentication).

Login name:
Enter your user name here.

Password:
Enter the relevant password here. The password is saved in encrypted form. For security reasons, the actual characters you type in this space are replaced by asterisks (*).

Send test email

When you click on the button, the program attempts to send a test email to the sender address to check the data entered.

9.7.1 Real-Time Protection email alerts

Avira Real-Time Protection can send alerts by email to one or more recipients for certain events.

Email alerts

If this option is enabled, Avira Real-Time Protection sends email messages with the most important information when a certain event occurs. This option is disabled as the default setting.

Email messages for the following events

The on-access scan detected a virus or malware

If this option is enabled, you always receive an email with the name of the virus or unwanted program and the affected file when the on-access scan detects a virus or an unwanted program.

Edit

The "**Edit**" button opens the "**Email template**" window in which you can configure the notification for an "On-access detection" event. You have the option of inserting text for the subject line and body of the email. You can use variables for this purpose. (See Email Template)

A critical error occurred in Real-Time Protection

If this option is enabled, you will receive an email whenever an internal critical error is detected.

Note
In this case, please inform our technical support and include the data given in the email. The specified file should also be sent for examination.

Edit

The "**Edit**" button opens the "**Email template**" window in which you can configure the notification for a "Critical error in Real-Time Protection" event. You have the option of inserting text for the subject line and body of the email. You can use variables for this purpose. (See Email Template)

Recipient(s)

Enter the email address(es) of the recipient(s) in this box. The individual addresses are separated by commas. The maximum length of all addresses together (i.e. the total character string) is 260 characters.

9.7.2 System Scanner email alerts

With certain events, the on-demand scan can send alerts and messages via email to one or more recipients.

Email alerts

If this option is enabled, the program sends email messages with the most important information when a certain event occurs. This option is disabled as the default setting.

Email messages for the following events

The scan reported a detection

If this option is enabled, you receive an email with the name of the virus or unwanted program and the affected file whenever the on-demand scan detects a virus or an unwanted program.

Edit

The "**Edit**" button opens the "**Email template**" window in which you can configure the notification for an "Scan detection" event. You have the option of inserting text for the subject line and body of the email. You can use variables for this purpose. (See Email Template)

End of scheduled scan

When the option is activated, an email is sent when a scan job has been performed. The email contains data on the point and duration of the scan job, on the folders and files scanned as well as on the viruses found and warnings.

Edit

The "**Edit**" button opens the "**Email template**" window in which you can configure the notification for the "End of scan" event. You have the option of inserting text for the

subject line and body of the email. You can use variables for this purpose. (See Email Template)

Add report file as attachment

If this option is enabled, the current report file of the System Scanner component is added to the email as an attachment when sending System Scanner notifications.

Recipient(s)

Enter the email address(es) of the recipient(s) in this box. The individual addresses are separated by commas. The maximum length of all addresses together (i.e. the total character string) is 260 characters.

9.7.3 Updater email alerts

The Updater component can send notifications by email to one or more recipients for specific events.

Email alerts

If this option is enabled, the Update component sends email messages with the most important data when a specific event occurs. This option is disabled as the default setting.

Email messages for the following events

No update necessary. Your program is up-to-date

If this option is enabled, an email is sent if the Updater has successfully made a connection to the download server but there are no new files available on the server. This means that your Avira product is up to date.

Edit

The "**Edit**" button opens the "**Email template**" window in which you can configure the notification for a "No update necessary" event. You have the option of inserting text for the subject line and body of the email. You can use variables for this purpose. (See Email Template)

Update completed successfully. New files have been installed

If this option is enabled, an email is sent for all updates performed: This may be a product update or an update of the virus definition file or of the scanning engine.

Edit

The "**Edit**" button opens the "**Email template**" window in which you can configure the notification for an "Update successful – new files installed" event. You have the option of inserting text for the subject line and body of the email. You can use variables for this purpose. (See Email Template)

Update finished successfully. A new product update is available

If this option is enabled, an email is only sent if an update of the scanning engine or virus definition file was performed without a product update, but a product update is available.

Edit

The "**Edit**" button opens the "**Email template**" window in which you can configure the notification for an "Update successful – product update available" event. You have the option of inserting text for the subject line and body of the email. You can use variables for this purpose. (see Email Template)

Update failed

If this option is enabled, an email is sent if the update has failed due to an error.

Edit

The "**Edit**" button opens the "**Email template**" window in which you can configure the notification for an "Update failed" event. You have the option of inserting text for the subject line and body of the email. You can use variables for this purpose. (See Email Template)

Add report file as attachment

If this option is enabled, the current report file of the Updater component is added to the email as an attachment when sending Updater notifications.

Recipient(s)

Enter the email address(es) of the recipient(s) in this box. The individual addresses are separated by commas. The maximum length of all addresses together (i.e. the total character string) is 260 characters.

Note
Alerts are always sent by email for the following events if an SMTP server and a recipient address have been configured for Updater notifications:
A product update is required for every further update of the program.
An update of the scanning engine or of the virus definition file could not be performed as a product update is necessary.
These alerts are sent irrespective of your email warning settings for the Update component.

9.7.4 Email template

In the **Email template** window you can configure the email notifications for the individual components to the enabled events. You can insert text of up to a maximum of 128 characters in the subject line and up to a maximum of 1024 characters in the message field.

The following variables can be used in the email subject and email message:

Globally acceptable variables

Variable	Value
Windows environment variables	The email notifications component supports all Windows environment variables.
%SYSTEM_IP%	IP address of the computer
%FQDN%	Fully qualified domain name
%TIMESTAMP%	Event time stamp: Time and date format as per the language settings of the operating system
%COMPUTERNAME%	NetBIOS computer name
%USERNAME%	Name of user accessing the component
%PRODUCTVER%	Product version
%PRODUCTNAME%	Product name
%MODULENAME%	Name of the component sending the email
%MODULEVER%	Version of the component sending the email

Specific component variables

Variable	Value	Component emails
%ENGINEVER%	Version of scan engine used	Realtime Protection System Scanner
%VDFVER%	Version of virus definition file used	Realtime Protection System Scanner
%SOURCE%	Fully qualified file name	Real-Time Protection
%VIRUSNAME%	Name of the virus or unwanted program	Realtime Protection
%ACTION%	Action performed after the detection	Realtime Protection
%MACADDR%	MAC address of the first registered network card	Realtime Protection
%UPDFILESLIST%	List of updated files	Updater
%UPDATETYPE%	Update type: Update of scan engine and virus definition file, or product update with update of scan engine and virus definition file	Updater
%UPDATEURL%	URL of download server used for update	Updater
%UPDATE_ERROR%	Update error in words	Updater

%DIRCOUNT%	Number of scanned directories	System Scanner
%FILECOUNT%	Number of files scanned	System Scanner
%MALWARECOUNT%	Number of viruses or unwanted programs detected	System Scanner
%REPAIREDCOUNT%	Number of infected files repaired	System Scanner
%RENAMEDCOUNT%	Number of infected files renamed	System Scanner
%DELETEDCOUNT%	Number of infected files deleted	System Scanner
%WIPECOUNT%	Number of infected files overwritten and deleted	System Scanner
%MOVEDCOUNT%	Number of infected files moved to quarantine	System Scanner
%WARNINGCOUNT%	Number of warnings	System Scanner
%ENDTYPE%	Status of scan: Terminated/Successfully completed	System Scanner
%START_TIME%	Start time of the scan: Start time of the update	System Scanner, Updater
%END_TIME%	End of the scan End of the update	System Scanner, Updater

%TIME_TAKEN%	Duration of scan in minutes Duration of the update in minutes	System Scanner, Updater
%LOGFILEPATH%	Path and file name of the report file	System Scanner, Updater

This manual was created with great care. However, errors in design and contents cannot be excluded. The reproduction of this publication or parts thereof in any form is prohibited without previous written consent from Avira Operations GmbH & Co. KG.

Issued Q4-2012

Brand and product names are trademarks or registered trademarks of their respective owners. Protected trademarks are not marked as such in this manual. However, this does not mean that they may be used freely.

AVIRA

live *free.*™

© 2012 Avira Operations GmbH & Co. KG. All rights reserved.
Errors and omissions excluded.

Avira Operations GmbH & Co. KG
Kaplaneiweg 1 | 88069 Tettnang
Germany

Telephone: +49 7542-500 0
Facsimile: +49 7542-500 3000
www.avira.com